

FORM PTO-1390  
(REV 10/95)

U. S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER

GRYN 202 - CAI

TRANSMITTAL LETTER TO THE UNITED STATES  
DESIGNATED/ELECTED OFFICE (DO/EO/US)  
CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR

09/720542

INTERNATIONAL APPLICATION NO.

PCT/FR00/01184

INTERNATIONAL FILING DATE

3 May 2000

PRIORITY DATE CLAIMED

03 May 1999

TITLE OF INVENTION

METHOD, SERVER SYSTEM AND DEVICE FOR MAKING SAFE A COMMUNICATION NETWORK

APPLICANT(S) FOR DO/EO/US

Michael STERN et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is the **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This express request to begin national examination procedures (35 U.S.C. 371(f) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(I).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
  - a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau.)
  - b. ☒ has been transmitted by the International Bureau.
  - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
  - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
  - b. ☐ have been transmitted by the International Bureau.
  - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
  - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An executed oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
  - ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information:
  1. International Search Report
  2. PTO FORM 1449

EXPRESS MAIL NO. EL 759723250 US Mailed December 22, 2000

09/720542

528 Rec'd PCT/PTO 22 DEC 2000

## BASIC NATIONAL FEE (37 CFR 1.492(A)(1) - (5)):

Search Report has been prepared by the EPO or JPO ..... \$860.00

International preliminary examination fee paid to USPTO (37 CFR 1.482)  
..... \$690.00No international preliminary examination fee paid to USPTO (37 CFR 1.482)  
but international search fee paid to USPTO (37 CFR 1.445(a)(2)) ... \$710.00Neither International preliminary examination fee (37 CFR 1.482) nor  
international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... \$1000.00International preliminary examination fee paid to USPTO (37 CFR 1.482)  
and all claims satisfied provisions of PCT Article 33(2)-(4) ..... \$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =

\$860.00

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30  
months from the earliest claimed priority date (37 CFR 1.492(e)).

\$

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE	
Total claims	29 - 20 =	9	x \$18/9.00	\$81.00
Independent	4 - 3 =	1	x \$80/40.00	\$40.00
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ \$250.00	\$

TOTAL OF ABOVE CALCULATIONS =

\$981.00

Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement  
must also be filed (Note 37 CFR 1.9, 1.27, 1.28).

\$490.50

SUBTOTAL =

\$490.50

Processing fee of \$130.00 for furnishing the English translation later than ☐ 20 ☐ 30  
months from the earliest claimed priority date (37 CFR 1.492(f)).

\$0

TOTAL NATIONAL FEE =

\$490.50

Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be  
accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property+

\$ 40.00

TOTAL FEES ENCLOSED =


\$530.50

Amount to be: refunded	\$
charged	\$

a. ☒ A check in the amount of \$490.50 (Filing Fee) and \$40.00 (Assignment Recordation Fee) to cover the above fees is  
enclosed.b. ☐ Please charge my Deposit Account No. 50-0624 in the amount of \$\_\_\_\_\_ to cover the above fees.  
A duplicate copy of this sheet is enclosed.c. ☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit  
Account No. 50-0624. A duplicate copy of this sheet is enclosed.NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a)  
or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

C. Andrew Im  
FULBRIGHT & JAWORSKI L.L.P.  
666 Fifth Avenue  
New York, NY 10103  
Customer No. 24972



SIGNATURE

C. Andrew Im December 22, 2000

NAME

40,657  
REGISTRATION NUMBER

EXPRESS MAIL NO. EL 759723250 US Mailed December 22, 2000

09/720542

528 Rec'd PCT/PTO 22 DEC 2000

CERTIFICATE OF EXPRESS MAIL

"Express Mail" mailing label # EL 759723250 US

Date of Deposit December 22, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and is addressed to: Commissioner of Patents and Trademarks, Washington D.C. 20231

Fani Kontopoulos

(Name of Depositor)

Fani Kontopoulos 12/22/00

(Signature of Depositor)

Fulbright & Jaworski L.L.P.  
666 Fifth Avenue  
New York, New York 10103

09/720542

528 Rec'd PGT/PTO 22 DEC 2000

GRYN 202 - CAI

CERTIFICATE OF EXPRESS MAIL	
"Express Mail" mailing label #	EL 759723263 US
Date of Deposit	December 22, 2000
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231	
Fani Kontopoulos	Name of Depositor
	
(Signature of Depositor)	

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicant(s) : Michael STERN et al.

Serial Number : To be Assigned

Filing Date : December 22, 2000

Priority  
International Appl. : PCT/FR00/01184

International  
Filing Date : May 3, 2000

Priority Date : May 3, 1999

For : METHOD, SERVER SYSTEM AND DEVICE FOR  
MAKING SAFE A COMMUNICATION NETWORK

---

Hon. Commissioner of Patents  
and Trademarks  
Washington, D.C. 20231

December 22, 2000

**PRELIMINARY AMENDMENT**

Sir:

Prior to examination please amend the application as follows:

002227 24502/60

IN THE SPECIFICATION

Page 1, before line 1, please insert -- **BACKGROUND OF THE INVENTION** --;

Page 8, before line 20, please insert -- **SUMMARY AND OBJECTS OF THE PRESENT INVENTION** --;

Page 20, before line 26, please insert -- **BRIEF DESCRIPTION OF THE DRAWINGS** --; and,

Page 21, before line 14, please insert -- **DETAILED DESCRIPTION OF THE EMBODIMENTS** --.

IN THE CLAIMS

Please cancel claims 1 - 29 and add the following new claims.

--30. (New) A method for distributively and dynamically securing a communications network, comprising the steps of:

interconnecting a network device between each computer equipment to be secured and the network;

intercepting communications between a computer equipment connected to said device and the network by said device;

obtaining information related to a user of said computer equipment by an authentication module associated with said device;

defining a security level of said device by said authentication module associated with said device;

transmitting said information related to the user and said security level of said device to an authentication management server connected to the network,

authenticating the user by said server in accordance with said information related to the user and said security level of said device;

transmitting security parameters from the server to each device on the network;

storing said security parameters by each device; and

processing said security parameters received from said server, thereby distributively and dynamically configuring the security of the network to address new modes of attack.--

--31. (New) The method of claim 30, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.--

--32. (New) The method of claim 31, further comprising the steps of:  
analyzing the messages related to said client/server applications by said device;

filtering the messages related to said client/server applications by said device; and

altering the messages related to said client/server applications by said device, thereby establishing a firewall.--

--33. (New) The method of claim 30, wherein said security parameters comprise a list of computer equipment which the user is authorized to communicate with.--

- 34. (New) The method of claim 33, further comprising the steps of:  
enabling said device to transmit messages between said computer equipment associated with the user and a computer equipment on said list; and  
blocking said device from transmitting messages between said computer equipment associated with the user and a computer equipment not on said list.--
- 35. (New) The method of claim 30, further comprising the steps of:  
customizing said device in accordance with a private encipherment key provided by said authentication module;  
storing public encipherment keys associated with private encipherment keys which customize the devices by said server.--
- 36. (New) The method of claim 35, wherein said security parameters comprise a list of computer equipment and the corresponding public encipherment key which the user is authorized to communicate with, in an enciphered manner.--
- 37. (New) The method of claim 36, further comprising the step of enciphering by said device communications between said computer equipment associated with the user and a computer equipment on said list by combining the private encipherment key of said device with the public encipherment key of said computer equipment on said list.--
- 38. (New) A system for distributively and dynamically securing a communications network secure, comprising:  
a network device interconnected between each computer equipment to be secured and the network, said device comprising:

at least two input/output interfaces for intercepting communications between a computer equipment connected to said device and the network;

an authentication module for obtaining information related to a user of said computer equipment and for defining a security level of said device;

a transmitter for transmitting said information related to the user and said security level of said device;

a storage device; and

a processor; and

an authentication management server connected to the network comprising:

a processor for authenticating the user in accordance with said information related to the user and said security level;

a management device for managing the authentications and the security levels;

a transmitter for transmitting security parameters to each device on the network; and

wherein said storage device is operable to store said security parameters and said processor of said device is operable to process said security parameters.--

--39. (New) The system of claim 38, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.--

--40. (New) The system of claim 39, wherein said processor said device comprises:  
an analyzer for analyzing the messages related to said client/server applications;





combining the private encipherment key of said device with the public encipherment key of said computer equipment on said list.--

- 46. (New) A server for distributively and dynamically securing a communications network, comprising:

a processor for processing information received from a plurality of network devices to authenticate users, each information being related to a user of a computer equipment connected to a device;

a management device for managing the authentication of the users; and

a transmitter for transmitting security parameters to said devices.--

- 47. (New) The server of claim 46, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.--

- 48. (New) The server of claim 46, wherein said security parameters comprise a list of computer equipment which a user is authorized to communicate with.--

- 49. (New) The server of claim 46, further comprising a storage device for storing all the public encipherment keys associated with private encipherment keys which customize said devices.--

- 50. (New) The server of claim 49, wherein said security parameters comprise a list of computer equipment and the corresponding public encipherment key which the user (U) is authorized to communicate with, in an enciphered manner.--

--51. (New) A device for securing a communications network secure, said device being interconnected between each computer equipment to be secured and said network, comprising:

at least two input/output interfaces for intercepting communications between a computer equipment connected to said device and the network;

an authentication module for obtaining information related to a user of said computer equipment and for defining the security level of said device,

a transmitter for transmitting information related to the user and said security level of said device to an authentication management server connected to the network;

a storage device for storing security parameters received from said server;

and

a processor for processing said security parameters.--

--52. (New) The device of claim 51, wherein said security parameters comprise a list of authorized computer client/server applications and information enabling each device to analyze messages related to said client/server applications.--

--53. (New) The device of claim 52, wherein said processor further comprising:

an analyzer for analyzing the messages related to said client/server applications;

a filter for filtering the messages related to said client/server applications;

and

an altering device for altering messages related to said client/server applications.--

- 54. (New) The device of claim 51, characterized in that the security parameters comprise a list of computer equipment which the user is authorized to communicate with.--
- 55. (New) The device of claim 54, wherein said processor is operable to permit messages to be transmitted between said computer equipment associated with the user and a computer equipment on said list, and operable to block messages between said computer equipment associated with the user and a computer equipment not on said list.--
- 56. (New) The device of claim 51, wherein said authentication module of said device is operable to provide a private encipherment key for customizing said device.--
- 57. (New) The device of claim 56, wherein said security parameters comprise a list of computer equipment and a corresponding public encipherment key which the user is authorized to communicate with, in an enciphered manner.--
- 58. (New) The device of claim 57, further comprising an encipherment module for enciphering communications between said computer equipment associated with the user and a computer equipment on said list by combining the private encipherment key of said device with the public encipherment key of said computer equipment on said list.--

### REMARKS

Applicants have canceled claims 1-29 and added new claims 30-58.

Applicants request that the foregoing amendment be entered prior to examination.

An early and favorable response is earnestly solicited.

No fee is believed to be due, however, should a fee become due the Commissioner is hereby authorized to deduct any fee associated with this filing from Deposit Account No. 500624.

Respectfully submitted,

**FULBRIGHT & JAWORSKI L.L.P.**

By

C. Andrew Im  
Reg. No. 40,657

666 Fifth Avenue  
New York, New York 10103  
(212) 318-3000

METHOD, SYSTEM, SERVER AND DEVICE FOR MAKING A  
COMMUNICATIONS NETWORK SECURE.

As an increasing number of companies are connecting to networks and in particular to Internet, security on computer networks becomes an important issue at the dawn of the twenty-first century. Many  
5 problems arise in companies and other organizations. These problems are usually referred to under the term of computer hacking; the people who are responsible for this are referred to as hackers.

This computer hacking has several facets. For  
10 example, it may be performed from outside or from the inside of 'the company', this term 'company' referring to a firm of an industrial or commercial nature, a government organization or any other association of interests. Further it may have different goals: alter,  
15 suppress, peruse data (read, change or delete); or prevent the computer network from operating properly (notably by remotely impairing the operation of the essential computers).

Before continuing, hacking methods shall have to  
20 be discussed, those that may be described as physical methods because they are based on physical characteristics of the computer systems.

The first and the most simple of these physical methods is what is called in computers, 'sniffing'.  
25 This corresponds to physical spying of connection cables. The hacker may thereby capture all the information which transits within this network. The hacker may obtain vital information: confidential information of any nature, network user passwords. He  
30 may also alter or delete these data.

002227 24502650



this user is authorized or not to access this file. The operating system makes this decision according to several criteria such as the owner of the file, the identification of the person who is requesting access  
5 to it, the access authorizations which have been determined by the owner. Therefore, the hacker must deceive the computer system in order to obtain the desired information by interfering with its logic.

It is practically unfeasible to create an  
10 exhaustive list of the methods used for hacking  
computer data or a network as these methods are so  
numerous. However, it should be stressed that they  
include common points after all and more particularly a  
common logic. General methods may thereby be  
15 established for opposing these hackers.

A first known method for defeating logical hacking consists in asking the user to provide a password in order to access data, a password which is acknowledged by the operating system. This password is a numerical value. Today, this remains the keystone of all security systems. Now, this is also its primary weak point: a hacker which knows the password of a user may access to this user's private data and may also impersonate this user which is far worst. Any action, error, mistake thereby committed by the hacker will therefore be wrongly ascribed to the hacked user.

Another known method for defeating hacking consists in encrypting data. This method is often considered as sufficient. This enciphering is presently carried out with software packages or electronic cards. The enciphering is based on using an encipherment key. This encipherment key is one of the weak points of this method. With this method, when two computers want to



communicate with each other, they must first be authenticated one by the other, i.e., use a common encipherment key. Presently this authentication process is numerical and is based either on a code typed in by the user or on a code logically generated by both computers. In this second case, unfortunately, both computers have to exchange a sequence of information until they mutually authenticate each other. It follows that a third computer entering and hacking this system may locate the generated code by perusing over this exchange of information. By doing this, it may have access to the transmitted data and may even usurp the identity of these hacked machines.

Data encryption is also used for making information contained on a computer data medium incomprehensible. In this case, the enciphering keys are generated in the same way as for encipherment of transmissions.

All enciphering methods presently used are based on mathematical algorithms. There are two encipherment algorithm classes: symmetrical algorithms and asymmetrical algorithms.

The symmetrical algorithm only uses one single enciphering key which therefore serves both for encrypting and decrypting data at the same time. Conversely, the asymmetrical algorithm uses two keys: a public key and a private key. In this second enciphering method, each user has two keys: a private key and a public key. His public key is known to all the other users. With it, the message may be encrypted but not decrypted. His private key is only known to him exclusively, and is unknown to the other users. With it, the enciphered message may be decrypted.

An asymmetrical system may be used for a key exchange protocol, i.e., a protocol enabling two users to agree on a symmetrical encipherment key to be used for the actual encipherment.

5        An example of such a protocol is detailed in US-4200770 et CA-1121480. As an example, and for a better understanding of the present document, this asymmetrical algorithm is described hereafter.

10        In the rest of the present document, the notation  $g^a[N]$  represents  $g$  to the power of  $a$ , modulo  $N$ .

15        Let  $A$  et  $B$  be two users of the algorithm. Each user has a confidential private key, for example ' $a$ ' for  $A$  et ' $b$ ' for  $B$ . The numbers  $g^a[N]$  and  $g^b[N]$  are known to all. Numbers  $g$  et  $N$  are fixed and chosen once  
20        and for all by  $A$  and  $B$ , in such a way that the multiplicative group for the successive powers of  $g$  modulo  $N$  has a large number of elements. Practically,  $N$  is chosen to be a very large prime number with for example about a hundred of decimal figures and such  
25        that  $(N-1)/2$  is prime, and that  $g$  is a primitive root modulo  $N$ , i.e. a generator for the multiplicative modulo  $N$  group.

30        When  $A$  wants to communicates with  $B$  in such a way as to be only understood by  $B$ ,  $A$  takes the public key of  $B$ :  $g^b$  and raises it to the power of ' $a$ ' (always modulo  $N$ ) which gives  $g^{(ba)}$  and thus provides the encipherment key for a symmetric algorithm.  $B$  is the only one able to understand the message by doing  
35         $(g^a)^b = g^{(ab)} = g^{(ba)} [N]$ .

40        This method works because there is no known algorithm for solving within a reasonable time, the ' $x$ ' equation:  $g^x = d [N]$  if  $N$  is very large.

Private keys ' $a$ ' and ' $b$ ' of  $A$  and  $B$  are usually

5       The encipherment algorithms presently used are very efficient. However, user authentication is not fully satisfying. In the case of direct authentication between two encipherment devices (therefore without any human intervention), a third encipherment device may  
10 manage to impersonate one of the other two devices and may thus access data on the other computer, as already mentioned. If the authentication requires that a code be typed in by the user on the keyboard of his computer, this code may be intercepted by a hacker or  
15 may be directly observed when it is typed in on the keyboard.

There is a third known method against hacking. This method is related to the protection of internal networks. In order to prevent intruders from penetrating into an internal network, several companies have introduced on the market, locks (more commonly called "firewalls" by computer specialists). This is a logical barrier between the company's network and a network which has not been made secure (for example, Internet). A lock is a device placed on a specific computer which prevents unauthorized accesses to information resources of the internal network. In other words, a lock operates like a gateway by monitoring information flowing in both directions. It is able to prevent certain external users from accessing certain data or software resources of the internal network. Thus, security problems of the internal network with regards to the outside world, are normally confined in

This lock, if it is properly used (alas, this is the case very rarely), is logically impenetrable. So, one will have to resort to another approach: for instance, the hacker will prevent the computer hosting the lock from properly operating by saturating it with messages sent to it profusely which will force this computer to exceed its information processing capabilities. If this computer is no longer running, the hacker may then penetrate into the network which is no longer made secure by the lock.

In order to defeat computer hacking in addition to the aforementioned prevention techniques, an attempt may also be made to find out who the author of this hacking is. It is possible to make use of the computer traces left behind him: opening of files, connections with servers... indeed, most computer handling operations leave digital traces in the operating systems. Unfortunately, it is rather easy to conceal these traces: usurping somebody's identity by using his password, borrowing a workstation so as to have someone else accused, are standard hacker techniques and are very easily implemented. Indeed today, user authentication is performed through his digital identifier but not by recognizing the physical person. As a result, one can never be absolutely certain of the identity of the user of a computer.

In order to increase the level of user authentication, several companies use bank authentication techniques: chip cards. New physical authentication methods like examining the retina or the  
5 finger prints of the user, exist but are still not very used because their reliability is still relatively unknown.

To summarize, it may be stated that the present methods for making a computer network safe have  
10 definite drawbacks. Indeed, they are based on operating systems having security loopholes, on imperfect authentication of the users. Furthermore, although security problems from outside the companies or the computerized organizations are feared essentially, it  
15 should also be considered, unfortunately, that very often these problems have an internal cause. A satisfactory method for making a computer network secure must therefore protect this network both from external and internal hacking.

20 The object of the present invention is to solve the aforementioned primary security problems of internal networks of a company or of any other interest group.

For this purpose, the present invention provides a  
25 method for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises the following steps:

- the step for interconnecting a device between each  
30 piece of computer equipment which should be made secure and the communications network,
- the step for intercepting communications between a piece of computer equipment provided with the

- the step for obtaining information related to a user of the piece of computer equipment by means of an authentication module associated with said device,
- the step for defining a security level of the aforementioned device by means of the authentication module associated with the device,
- the step for transmitting information related to the user and the security level of the device to an authentication management sever connected to the network,
- the step for processing by means of the server, said information related to the user and the said security level of the device and for authenticating the user with the help of such information,
- the step for managing authentications and security levels by means of the authentication management server,
- the step for transmitting security parameters from the server to the network devices,
- the step for storing by means of the devices, said security parameters from the server,
- the step for processing by means of the devices, said security parameters from the server.

This enables the identity of the user of the device according to the invention to be known at any time. Thus, the user authentication is performed in two steps: the authentication module sends information on the user (for example the fact that he has been properly authenticated by means of such a chip card, or

still by his finger prints or a picture of his retina). This information is specific to each user and is sent to the authentication management server. This server then checks whether the relevant user is authorized to use the network component equipped with the device according to the invention which has just sent the authentication request. The server then sends back to the device according to the invention, its consent or it reports that the user is not authorized to use said network component.

This method provides distributed and dynamic security on a computer network. Indeed, security is supported by interconnected devices between each computer equipment which should be made secure and the communications network. The security of these devices is managed by a central server which receives information from all these devices. The server may now choose an overall security policy which will then be applied at each of the devices.

This security is configurable and it may develop over time according to new needs or modes of attack.

Indeed, a more flexible management of the network is achieved by having this list of security parameters sent by an authentication management server. The sent information may be very simply changed on the authentication server. User access authorization may thereby be changed easily.

Specifically, it should be noted that the security parameters depend on:

- the user,
- the network component which he desires to use,
- the security level which he has selected,
- the date and time,

- the network status
- and all the security parameters already provided to the devices.

On the other hand, an embodiment using a data  
5 medium specific to each user and containing the  
aforementioned list does not provide simple management  
of the network: any change in the security parameters  
of the user requires the changing of data contained in  
his private data medium.

10           The address of the authentication management  
server is either provided by the user of the device or  
already stored in the device.

Advantageously, the security parameters comprise:

- 15       -     a     list     of     authorized     computer     client/server  
       applications,  
       -     information     enabling     the     devices     to     analyze     the  
       messages     related     to     said     client/server  
       applications.

Advantageously, the method according to the  
20 invention consists of:

- the step for analyzing by means of the device, the messages related to said client/server applications,
- the step for filtering by means of the device, the messages related to said client/server applications,
- the step for changing by means of the device, the messages related to said client/server applications.

30           The filtering of the messages may thus eliminate  
information packets which do not comply with the  
communications protocol used on the computer network.  
Indeed, an information packet of a specific



5

10

15

Thus, an application may already be well characterized by a simple list of communication ports.

25

30

This method provides a lock managed by a server and distributed over all the network. In addition, this lock has particular properties for each piece of computer equipment equipped with the device.

- a list of pieces of computer equipment which the user is authorized to communicate with.

- the step for having the device transmit messages between the piece of computer equipment to which it is connected and the computer equipment which the user is authorized to communicate with,
- 15 - the step for having the device block the messages between the piece of computer equipment to which it is connected and the computer equipment which the user is unauthorized to communicate with.

With this method, a system may be designed for partitioning the network components.

- the step for customizing the device with a private encipherment key provided by means of the authentication module,

- 5           Advantageously, the security parameters further  
comprise:

- Advantageously, the method according to the  
15 invention further comprises the following steps:

- In this operating mode, each device is customized by a private encipherment key allowing an encipherment key exchange protocol to be executed. This private key is associated with a public encipherment key registered in the list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way.

The present invention provides a system for distributively and dynamically making a communications



applications,

- information enabling the devices to analyze the messages related to said client/server applications.

5 Advantageously, the processing means of the device comprise:

- means for analyzing the messages related to said client/server applications,
- means for filtering the messages related to said client/server applications,
- 10 - means for changing messages related to said client/server applications.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with.

15 Advantageously, said processing means of the device comprise:

- means for allowing messages to be transmitted between the piece of computer equipment to which the device is connected and the computer equipment which the user is authorized to communicate with,
- 20 - means for blocking messages between the piece of computer equipment to which said device is connected and computer equipment which the user is not authorized to communicate with.

25 Advantageously, the system according to the invention comprises:

- an authentication module associated with the device customized by means of a private encipherment key which customizes the device with which it is associated,
- 30 - a server storing all the public encipherment keys associated with private encipherment keys which

002227 24502/60

customize the devices.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user is authorized to communicate with, in an enciphered way.

Advantageously, the devices comprise:

- an encipherment module for enciphering communications by combining the private encipherment key of the device with the public encipherment key of the computer equipment which the user is authorized to communicate with, in an enciphered way.

The present invention provides a server for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises:

- processing means for processing information from a device and related to a user of a piece of computer equipment to which this device is connected,
- said processing means enable the user to be authenticated with the help of said information,
- management means for managing the authentications,
- transmission means for transmitting the security parameters to the devices of the network.

Advantageously, the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server

applications.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with.

5       Advantageously, the server according to the invention comprises:

- storage means for storing all the public encipherment keys associated with the private encipherment keys which customize the devices.

10       Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with, in an enciphered way,
  - the public encipherment key of each piece of computer equipment which the user is authorized to communicate with, in an enciphered way.
- 15

The present invention provides a device for making a communication network secure, interconnected between each piece of computer equipment which is to be made secure and said network and characterized in that it comprises:

20

- two input/output interfaces for intercepting communications between a piece of computer equipment to which it is connected and its communications network,
  - an authentication module for obtaining information related to a user of the piece of computer equipment to which said device is connected and for defining the security level of said device,
  - means for transmitting information related to the user and the security level of the device, to an authentication management server,
  - storage means for storing security parameters from
- 25
- 30

the server,

- processing means for processing said security parameters from the server.

Advantageously, the security parameters comprise:

- 5 - a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

10 Advantageously, said processing means of the device comprise:

- means for analyzing the messages related to said client/server applications,
- means for filtering the messages related to said client/server applications,
- 15 - means for changing the messages to said client/server applications.

Advantageously, the security parameters comprise:

- a list of pieces of computer equipment which the user is authorized to communicate with.

20 Advantageously, said processing means of the device comprise:

- means for allowing messages to be transmitted between the piece of computer equipment to which the device is connected and computer equipment which the user is authorized to communicate with,
- 25 - means for blocking messages between the piece of computer equipment to which the device is connected and computer equipment which the user is unauthorized to communicate with.

30 Advantageously, the authentication module associated with said device provides:

- a private encipherment key which customizes said





Fig. 3 shows a general diagram of a second embodiment of the device according to the invention.

Fig. 4 shows the second embodiment of the device according to the invention when it is implemented in a computer.

Fig. 5 shows the second embodiment of the device according to the invention when it is on the outside of a computer component as an external module.

Fig. 6 shows an embodiment of the encryption module 7.

Figs. 7 and 8 show an embodiment of the device according to the invention when it is miniaturized in a chip.

Fig. 1 shows a general diagram of a network made secure through the invention. This may be an internal network of a company, a public network like Internet or a mixed network, i.e. one or more internal or external networks connected with each other. This network is made up of 7 computer components noted as A, B, C, D, E, F, G which may be a computer, a computer server, a portable computer, a printer server, a printer... These computer components are equipped with the device according to the invention. The network has an authentication management server S. Two users of this network have been illustrated: a user U using component A of the network and a user U' who may use component B of the network.

Fig. 2 shows a general diagram of a first embodiment of the device according to the invention, made up of a microprocessor 1, connected through a data bus 2 to a memory 3, to two input/output interfaces 8 and 9, to a user authentication module 6 and to an encryption module 7.





The authentication management server then sends to the device according to the invention which equips computer A, the list of authorized addresses for user U as well as their public keys and the list of authorized communications ports for this user. This sending always occurs in an encrypted way but this time, by using key  $g^{su} [N]$  (where 'u' represents the user's private key for encrypting communications with the authentication management server S). The microprocessor 1 of the electronic card 10 placed in computer A then stores this list.

30           In order not to impair the network's operation,  
the microprocessor 1 calculates the encryption keys  
 $g^{ab} [N]$  (where 'b' is the private key of any other  
network component B) when it has nothing else to do.





Now, under the assumption that the user of computer A desires to personally encrypt data on his computer, he sends the data to be encrypted to the microprocessor 1 with the help of a software package which is not part of the invention. These data are then encrypted with the help of the DES chip of the encryption module 7 and of one of the personal encryption keys contained in the chip card of the user (the encryption key is selected by the software package). Decrypting works in the same way.

If communications between each pair of network components equipped with the device according to the invention are not customized, the microprocessor 1 does not have to calculate the encryption keys required for encrypting communications because they are then contained on each data medium 5, in the list of private encryption keys.

30 By having several chip cards, the user may  
therefore have access to different security levels on  
different computer groups. The security parameters  
transmitted by the server of course depend on the



required security level.

In another embodiment of the invention illustrated in Fig. 5, where each device according to the invention is not placed in a computer, but placed as an independent module on the network, it may be contemplated that the device according to the invention is then not customized by a private encryption key contained in memory 3 but by a private encryption key contained on the data medium 5 specific to each user; this key is read as soon as the user is authenticated by the authentication module. In this embodiment illustrated in Fig. 5, the device according to the invention is made up of an electronic card 13 bearing the microprocessor 1 connected through several buses 2 to: a memory 3, an encryption module 7, both input/output interfaces 8 and 9 which, in this embodiment, are network interfaces providing for example the Ethernet wrapping in the case of an Ethernet network. The data reader 4 may further be coupled with an authentication module 6 as a chip card reader which may be placed on the electronic card 13 or which may be external to the above described module according to another embodiment.

The components used in this embodiment may be those used in the first embodiment.

Operation of the module is identical to the operation of the device according to the invention as described in the first embodiment except as regards the private encryption key. This key must be read as soon as the user is identified with the help of the identification module 6 so that the encryption keys  $((g^{ab} [N]))$  may be calculated.

It should be noted that the chip card reader may

be replaced with a finger print reader or with the reader for the retina of the user. The address of the authentication management server S is then contained in memory 3 as well as its public encryption key. When the user is authenticated with the help of the authentication module 6, this module 6 then has the digital information on the user, which it sends to the microprocessor 1. The latter then uses part of this information (for example the first 128 bits) in order to form the private key 'u' of the user for encrypting communications with the authentication management server S.

Everything then takes place as in the case of the chip card reader except for the fact that the user must report when he ceases using the device according to the invention, for example by pressing on a button.

Fig. 6 illustrates in more details an embodiment of the encryption module 7, part of the device according to the invention. Now, 12 DES chips arranged in columns of four are inserted; these chips are referenced by notation  $P_{i,j}$  where  $i$  is the index of the column and  $j$  that of the line. Two mixers M1 and M2 are also added.

This encryption module operates with any block encoding algorithm, whereby the latter may be performed by a software package or by a specific hardware device. In order to simplify the test and to emphasize the analogy with algorithms of the DES triple type detailed later on, an example based on the use of a DES chip will be discussed.

The DES algorithm operates with a 56 bit key on messages cut up into 64 bit packets. Triple DES is an encoding algorithm based on the use of three successive

5

10

20

25

30

10

15

25

30

general public, or  $K_{1,1} = K_{1,2} = K_{1,3} = K_{1,4}$  and  $K_{2,1} = K_{2,2} = K_{2,3} = K_{2,4}$ . The key will then have 128 or 256 bits.

On a same basis, it is possible to work on large  
5 blocks grouping an arbitrary number of elementary blocks on which will act a DES or any other block encoding algorithm.

In a third preferred embodiment where each device according to the invention may be placed either in a  
10 computer or in an independent module, the device is then miniaturized in a chip.

The third preferred embodiment is described in Figs. 7 and 8.

The device according to the invention is then made  
15 up of an electronic card 13 bearing a chip 100 connected through several buses 120, 121, 122, and 123 with:

- a memory 3,
- two physical connectors 108 and 109, which in this  
20 preferred embodiment, are two network connectors (for example ARJ45) or a network connector and a connector to an internal bus of the computer (for example, a PCI bus),
- a data reader 4 may further be coupled with an  
25 authentication module 7 as a chip card reader which may be placed on the electronic card or which may be external to the above described module according to another embodiment.

The components (3, 4 and 6) used in this preferred  
30 embodiment may be those used in the first embodiment.

Bus 120 is a serial bus (RS 232), busses 121, 122 and 123 are 32 bit buses.

Connectors 108 and 109 are standard connectors

002221 2452460



The operation of the module is identical to the operation of the invention as described in the first or second preferred embodiment: everything depends on the private encryption key which may be placed either in  
5 chip 100 (as in the first embodiment) or provided by the user (as in the second embodiment).

It is well understood that the different embodiments described above are purely illustrative and non-limiting and that many alterations may be made to  
10 them without however departing from the scope of the invention.

It should be noted that the chip card reader may be replaced with a finger print reader or with a reader for the retina of the user.

097094-1330

CLAIMS

1. A method for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises the following steps:

- 5     - the step for interconnecting a device (D) between each computer equipment which must be made secure and the communications network,
- the step for intercepting communications between a  
10     piece of computer equipment (A) provided with device (D) and the communications network by means of said device to which this piece of equipment is connected,
- the step for obtaining information related to a  
15     user (U) of the piece of computer equipment (A) by means of an authentication module (6) associated with device (D),
- the step for defining a security level of the  
20     device (D) by means of the authentication module (6) associated with device (D),
- the step for transmitting information related to  
25     the user (U) and the security level of the device (D) to an authentication management server (S) connected to the network,
- the step for processing by means of the server  
      (S), said information related to the user and to  
      said security level of the device and for  
      authenticating the user with the help of said  
      information,
- 30     - the step for managing the authentications and the security levels by means of the authentication management server (S),



- (this method enables a distributed and dynamical security to be obtained on a computer network (R), this security is configurable and may develop over time, depending on new needs or new modes of attack)

15       - a list of authorized computer client/server applications,  
      - information enabling the devices to analyze the messages related to said client/server applications.

- the step for analyzing by means of the device (D), the messages related to said client/server applications,

- 30 (this method allows a lock to be obtained (commonly called a firewall) managed by a server and distributed over all the network. This lock further has particular properties for each piece of computer equipment

equipped with the device)

4. A method according to claim 1, characterized in that the security parameters further comprise:

- a list of pieces of computer equipment which the user (U) is authorized to communicate with.

5. A method according to claim 4, characterized in that it further comprises the following steps:

- the step for allowing the device (D) transmit messages between the piece of computer equipment (A) and computer equipment which the user (U) is authorized to communicate with,
- the step for blocking with the device (D) messages between the piece of computer equipment (A) and computer equipment which the user (U) is not authorized to communicate with.

(this method enables a partitioning system to be designed for the network components)

6. A method according to claim 1, characterized in that it further comprises the following steps:

- the step for customizing the device (D) with the help of a private encipherment key provided by means of the authentication module (6),
- the step for storing by means of the server (S), all public encipherment keys associated with private encipherment keys which customize the devices.

7. A method according to claim 6, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user (U) is

authorized to communicate with, in an enciphered way.

8. A method according to claim 7, characterized in that it further comprises the following steps:

- 5 - the step for enciphering by means of device (D), communications by combining the private encipherment key of said device (D) with the public encipherment key of the piece of computer equipment which the user (U) is authorized to  
10 communicate with, in an enciphered way.

(this method provides encipherment of communications between two devices. This encipherment depends on each pair of devices)

9. A system for distributively and dynamically  
15 making a communications network secure, notably of the Internet type, characterized in that it comprises:

- a device (D) interconnected between each piece of computer equipment which is to be made secure and the communications network,
- 20 - said device including two input/output interfaces for intercepting communications between a piece of computer equipment (A) to which it is connected and the communications network,
- said device further including an authentication  
25 module (6) for obtaining information related to a user (U) of the computer equipment (A) and for defining a security level of said device,
- said device including means for transmitting information related to the user (U) and to the  
30 security level of the device,
- an authentication management server (S) connected to the network including processing means for processing said information and said security

002221 24502760

level and for authenticating the user with the help of said information,

- said server including management means for managing the authentications and the security levels,
- said server (S) including means for transmitting security parameters, to the devices of the network,
- said devices (D) including storage means for storing said security parameters,
- said devices (D) including processing means for processing said security parameters.

10. A system according to claim 9, characterized in that the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

11. A system according to claim 10, characterized in that the processing means of the device comprise:

- means for analyzing the messages related to said client/server applications,
- means for filtering the messages related to said client/server applications,
- means for altering messages related to said client/server applications.

12. A system according to claim 9, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with.

13. A system according to claim 12, characterized in that said processing means of the device further comprise:

- means for allowing messages to be transmitted between the piece of computer equipment (A) and computer equipment which the user (U) is authorized to communicate with,
- 5 - means for blocking messages between computer equipment (A) and computer equipment which the user (U) is not authorized to communicate with.

14. A system according to claim 9, characterized in that

- 10 - the authentication module associated with the customized device by means of a private encipherment key which customizes the device with which it is associated,
- the server (S) stores all the public encipherment  
15 keys associated with private encipherment keys which customize the devices.

15. A system according to claim 14, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is  
20 authorized to communicate with, in an enciphered way,
- the public encipherment key of each piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered  
25 way.

16. A system according to claim 15, characterized in that the device further comprises:

- an encipherment module for enciphering communications by combining the private encipherment  
30 key of device (D) with the public encipherment key of the piece of computer equipment with which the user (U) is authorized to communicate with, in an enciphered way.

002221 24502/50

17. A server for distributively and dynamically making a communications network secure, notably of the Internet type, characterized in that it comprises:

- processing means for processing the information  
5 from a device (D) and related to a user (U) of a piece of computer equipment (A) to which this device (D) is connected,
- said processing means enabling the user (U) to be identified with the help of said information,
- 10 - management means for managing the authentications,
- transmission means for transmitting security parameters to the network devices.

18. A server according to claim 17, characterized in that the security parameters comprise:

- 15 - a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server applications.

20 19. A server according to claim 17, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with.

20. A server according to claim 17, characterized  
25 in that it comprises:

- storage means for storing all the public encipherment keys associated with private encipherment keys which customize the devices.

21. A server according to claim 20, characterized  
30 in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,

- the public encipherment key of each piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered way.

5        22. Device for making a communications network secure, interconnected between each piece of computer equipment which is to be made secure and said network and characterized in that it comprises:

- 10        - two input/output interfaces for intercepting communications between computer equipment (A) to which it is connected and the communications network,
- 15        - an authentication module (6) for obtaining information related to a user (U) of the computer equipment (A) and for defining the security level of said device,
- means for transmitting information related to user (U) and the device's security level to an authentication management server (S),
- 20        - storage means for storing security levels from the server (S),
- processing means for processing said security levels from the server (S).

25        23. A device according to claim 22, characterized in that the security parameters comprise:

- a list of authorized computer client/server applications,
- information enabling the devices to analyze the messages related to said client/server
- 30        applications.

24. A device according to claim 23, characterized in that said processing means of the device comprise:

- means for analyzing the messages related to said

client/server applications,

- means for filtering the messages related to said client/server applications,
- means for altering messages related to said client/server applications.

5

25. A device according to claim 22, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with.

10

26. A device according to claim 25, characterized in that said processing means of the device comprise:

- means for allowing messages to be transmitted between a piece of computer equipment (A) and the computer equipment which the user (U) is authorized to communicate with,

15

- means for blocking messages between a piece of computer equipment (A) and computer equipment which the user (U) is unauthorized to communicate with.

20

27. A device according to claim 22, characterized in that the authentication module associated with said device further provides:

- a private encipherment key which customizes said device(D).

25

28. A device according to claim 27, characterized in that the security parameters further comprise:

- a list of computer equipment which the user (U) is authorized to communicate with, in an enciphered way,

30

- the public encipherment key of each piece of computer equipment which the user (U) is authorized to communicate with, in an enciphered way.



29. A device according to claim 28, characterized in that it further comprises:

- an encipherment module for enciphering communications by combining the private encipherment key of said device (D) with the public encipherment key of the computer equipment which the user (U) is authorized to communicate with, in an enciphered way.



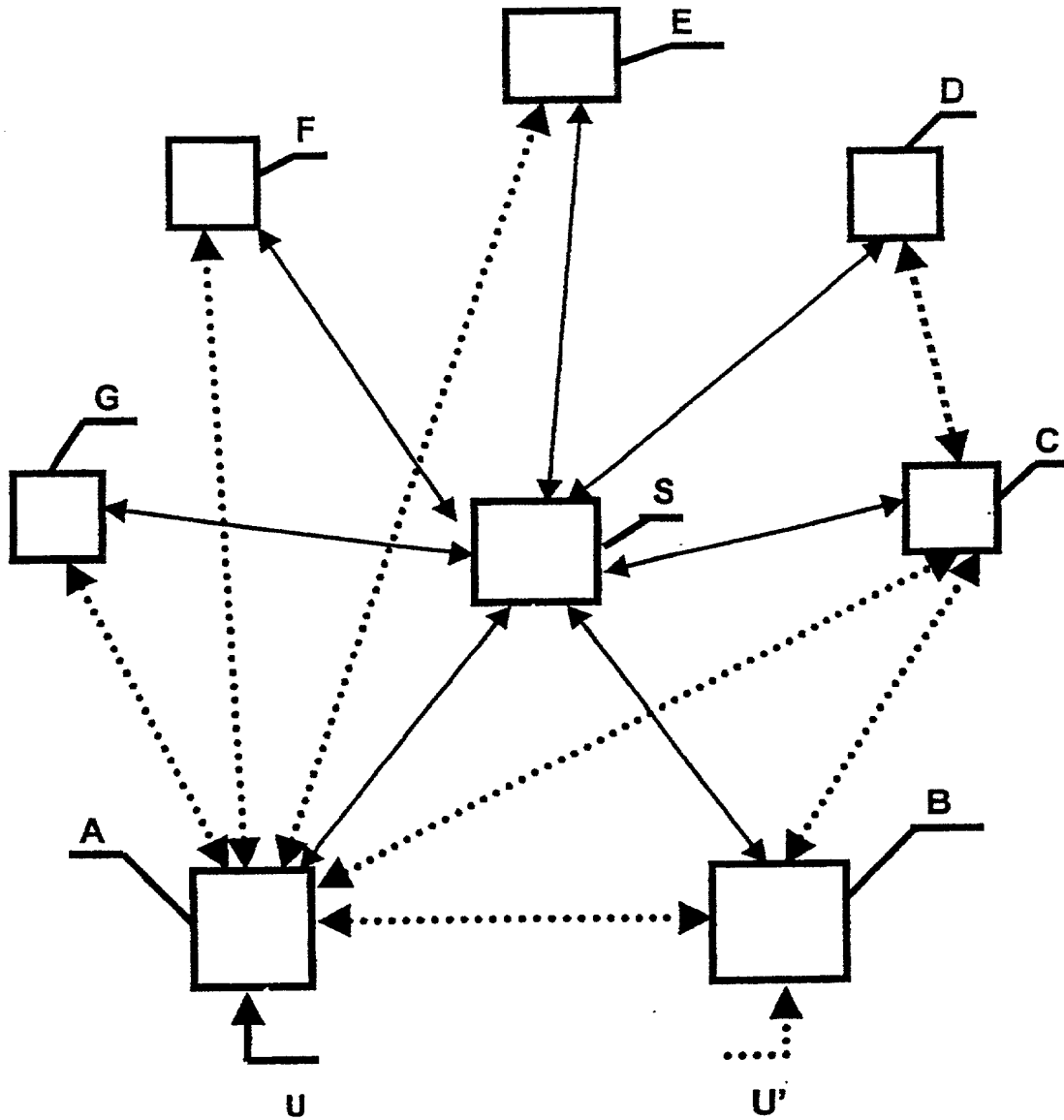
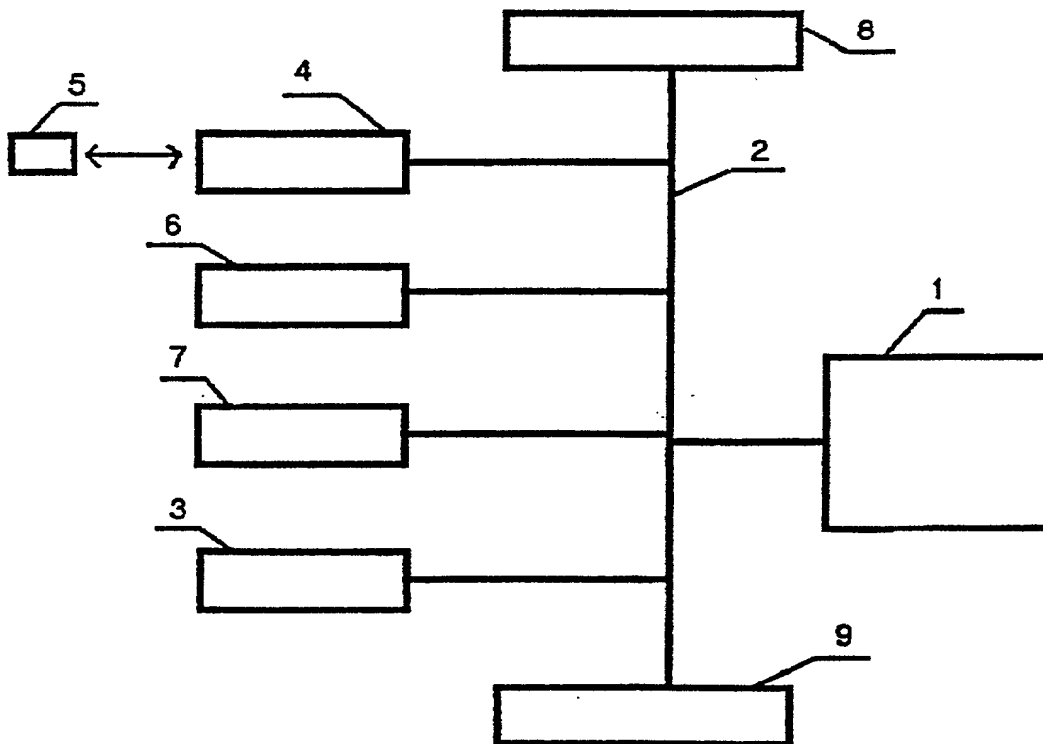
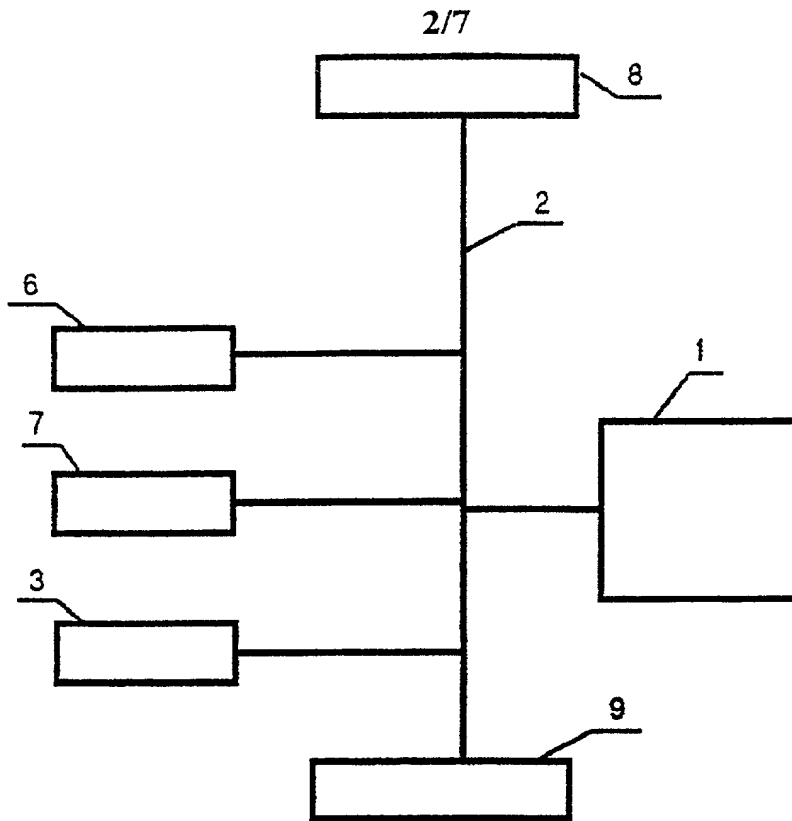


FIG.1



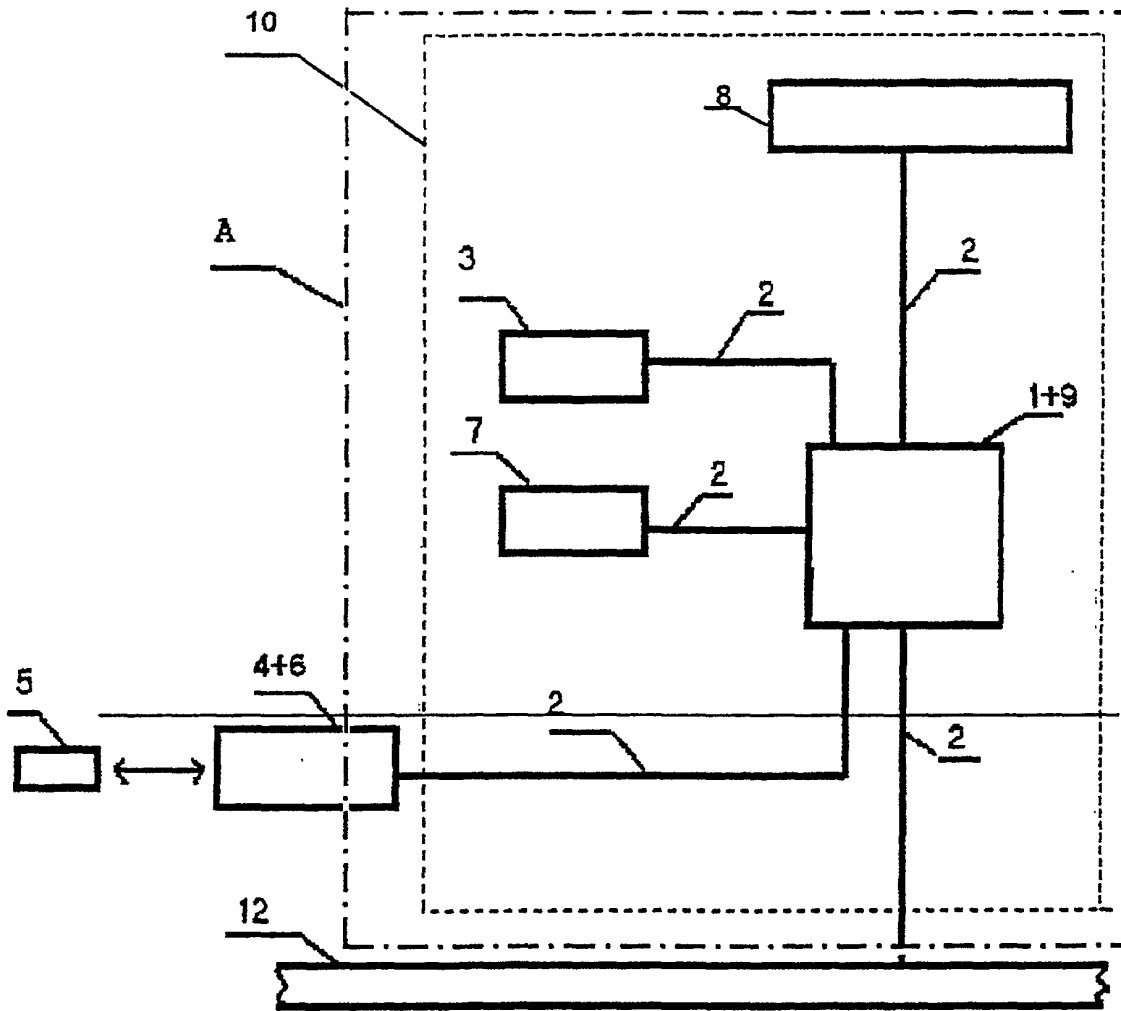


FIG. 4

4/7

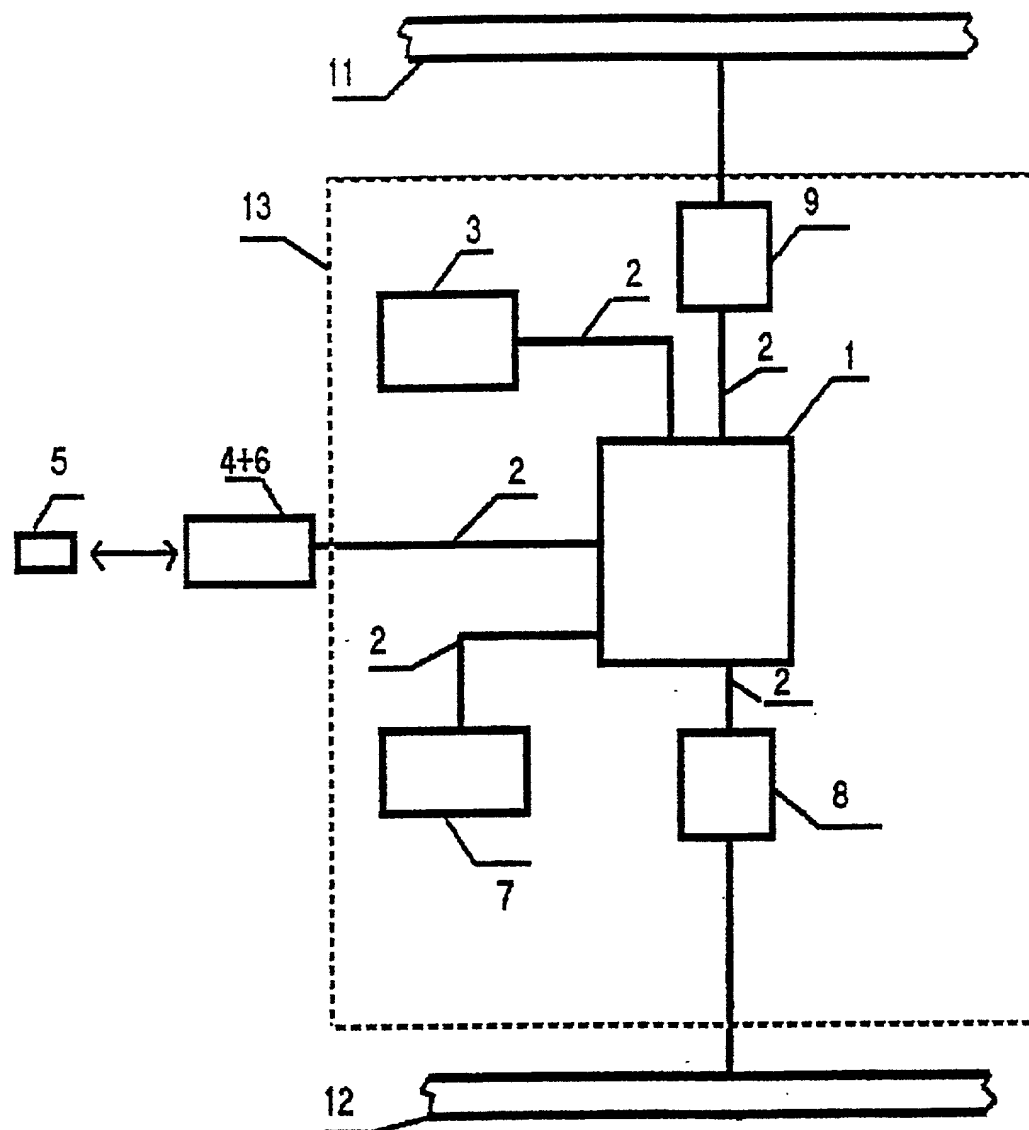


FIG. 5

5/7

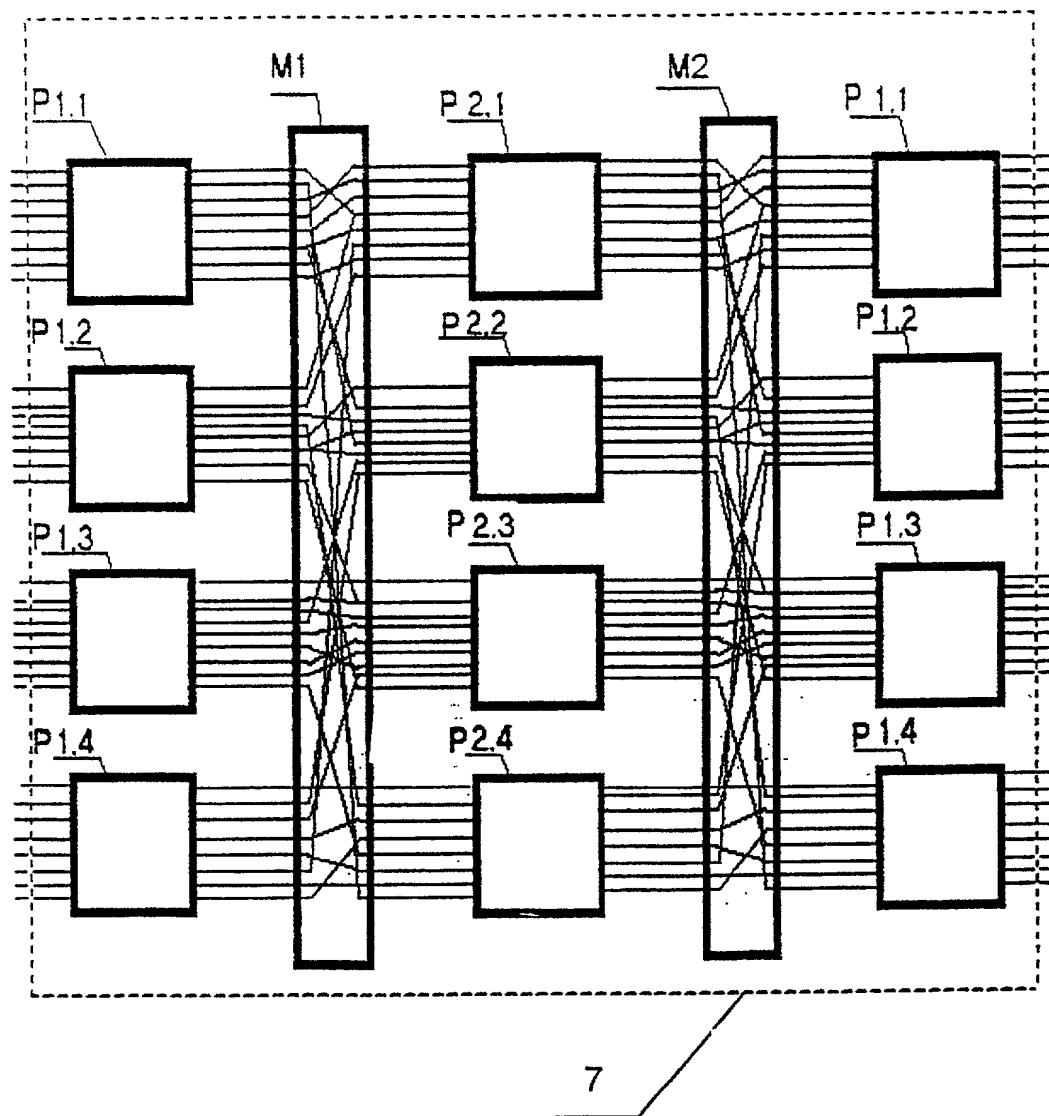


FIG. 6

6/7

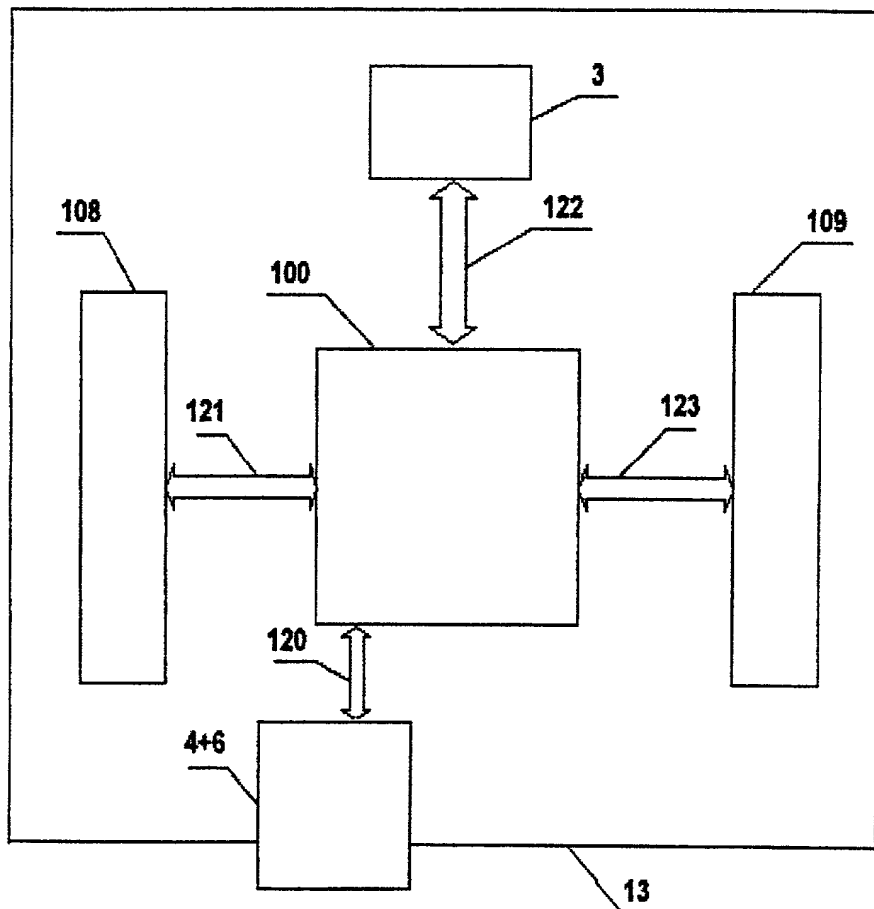


FIG. 7



7/7

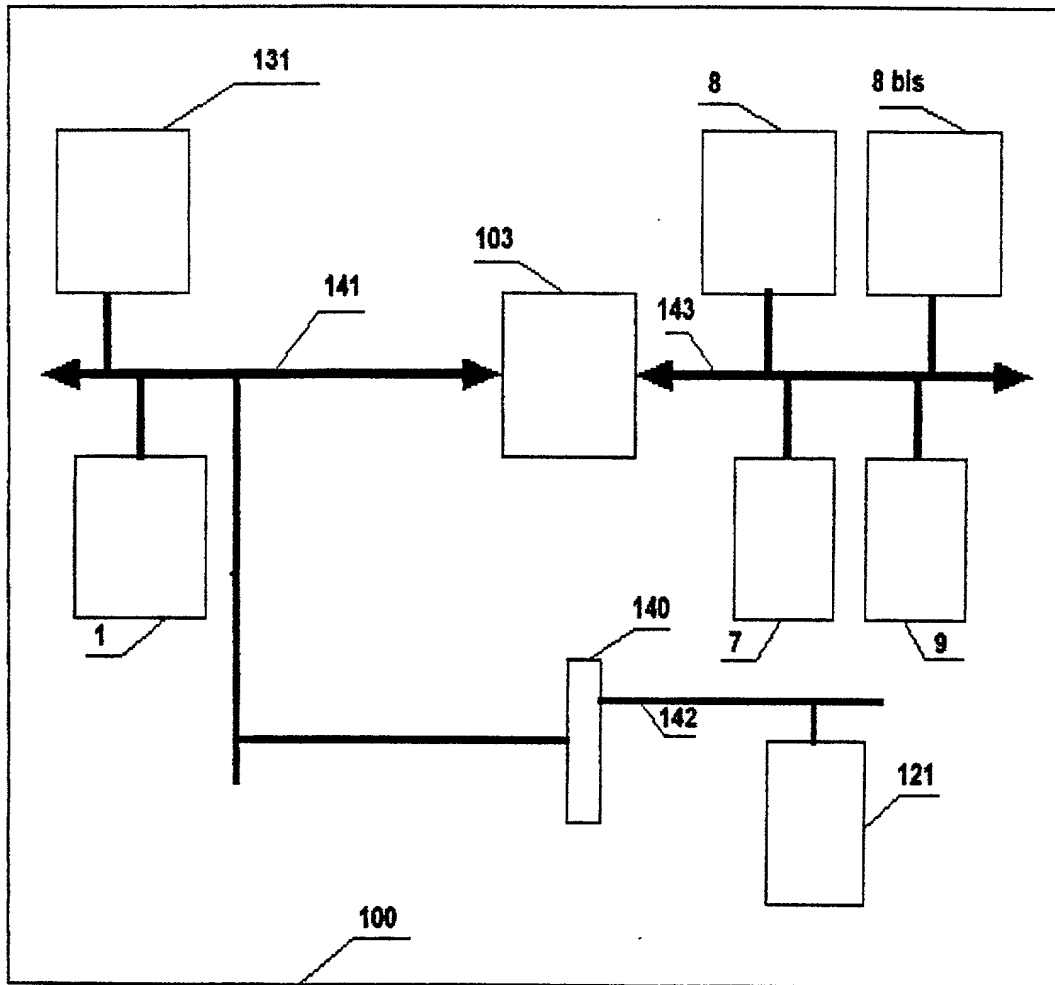


FIG.8

**DECLARATION FOR PATENT APPLICATION**

As a below named inventor, I hereby declare that:

My resident, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **"METHOD, SERVER SYSTEM AND DEVICE FOR MAKING SAFE A COMMUNICATION NETWORK"**, the specification of which

☐ is attached hereto.

☐ was filed on \_\_\_\_\_ as application Serial No. \_\_\_\_\_

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, 1.56(a).

**Foreign Priority Applications**

I hereby claim foreign priority benefits under Title 35, United States Code 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

**Priority Claimed**

<u>99/05609</u>	<u>FR</u>	<u>03 May 1999</u>	Yes (X) No ( )
(Number)	(Country)	(Day/Month/Year Filed)	

_____	_____	_____	Yes (X) No ( )
(Number)	(Country)	(Day/Month/Year Filed)	

**U.S. Priority Applications**

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims

p)

JCS

M.S

09720542 122000

of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

<u>PCT/FR99/01184</u>	<u>03 May 2000</u>	<u>Pending</u>
(Serial No.)	(Filing Date)	(Status-patented/pending/abandoned)

### **Power of Attorney**

I hereby appoint the following attorneys and patent agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: John E. Lynch, Reg. No. 20,940; Peter F. Felfe, Reg. No. 20,297; Norman D. Hanson, Reg. No. 30,946; John A. Bauer, Reg. No. 32,554; James Zubok, Reg. No. 38,671; James R. Crawford, Reg. No. 39,155; C. Andrew Im, Reg. No. 40,657; David Rubin, Reg. No. 40,314; and William C. Coppola, Reg. No. 41,686; my attorneys with full power of substitution and revocation. Address all telephone calls to **C. Andrew Im (212) 318-3000**. Address all correspondence to:

**FULBRIGHT & JAWORSKI L.L.P.**  
**666 Fifth Avenue**  
**New York, New York 10103**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

(1) Michael STERN

Full Name/Sole or First Inventor

Signature

Date

15.12.2000

Residence: 60, rue Lecourbe

F-75015 Paris, France

Post Office Address: Same as Above

Citizenship: French

(2) Nicolas STEHLE

Full Name/Second Inventor

Signature

Date 15/12/00

Residence: 288, rue de Vaugirard

F-75015 Paris, France FLX

Post Office Address: Same as Above

Citizenship: French

(3) Jean-Luc STEHLE

Full Name/Third Inventor

Signature

Date

Residence: 300, rue de Vaugirard

F-75015 Paris, France FLX

Post Office Address: Same as Above

Citizenship: French